MULTIMEDIA UNIVERSITY

STUDENT ID NO

MULTIMEDIA UNIVERSITY

FINAL EXAMINATION

TRIMESTER 2, 2016/2017 SESSION

TSN 3251 / TSC 2211 – COMPUTER SECURITY

(All Sections / Groups)

4 MARCH 2017
9.00 a.m. – 11.00 a.m.
(2 Hours)

INSTRUCTIONS TO STUDENTS

1. This Question paper consists of 3 printed pages including cover page with 5 questions only.

2. Attempt **ALL** questions. All questions carry equal marks and the distribution of marks for each question is given.

3. Please write all your answers in the Answer Booklet provided

Question 1

a) What is a Structured Query Language (SQL)? (2 marks)
b) Describe in brief how SQL injection attacks work. (2 marks)
c) An HTML login form consists of two fields: username and password. When users key in their usernames and passwords, the following SQL will be generated to validate their identities.

$query = "SELECT * from login where name = '$_POST[username]' and pass = '$_POST[password]' "

Use tautology attack to compromise the login. (2 marks)
d) What are inferential attacks? (2 marks)
e) Items need to couriered are as shown in the following table of a database. The expensive item is the Jewelry.

Box	Item_ID	Item	Class
A	1001	Jewelry	Manager
A	1002	Documents	Clerk
C	1003	Toys	Clerk
A	1004	Stationaries	Clerk

The clerk is only able to access the table to view and modify non-expensive items. However, using inferential attack, the clerk is able to figure out an expensive item in Box A. Explain how this is possible with inferential attack? (2 marks)

Question 2

a) A cipher text $\begin{bmatrix}20\\5\end{bmatrix}$ is obtained using Hill Cipher. Decrypt the cipher text with the following information. The plaintext should be letters such that A=0, B=1 and so forth.
The original matrix is $\begin{bmatrix}5 & 8\\2 & 3\end{bmatrix}$. The inverse of a matrix A $\begin{bmatrix}a & b\\c & d\end{bmatrix}$ is
$A^{-1} = \frac{1}{|A|}\begin{bmatrix}d & -b\\-c & a\end{bmatrix}$ and $|A|$ = ad-bc. (5 marks)

b)

Table for Odd Positions

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
a	d	g	j	m	p	s	v	y	b	e	h	k	n	q	t	w	z	c	f	i	l	o	r	u	x

Table for Even Positions

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
n	s	x	c	h	m	r	w	b	g	l	q	v	a	f	k	p	u	z	e	j	o	t	y	d	i

Using the tables for odd and even positions as shown above, encrypt the following words. (2 marks)
Prepare for war

c) Explain how the encryption method, as shown in (b), solves the weakness of mono-alphabetic ciphers such as Caesar cipher. (2 marks)
d) What is the main key to decrypt Scytale cipher? (1 mark)

Continued...

Question 3

The following questions are related to Advanced Encryption Standard (AES).

a) What is the input block size for AES? (1 mark)
b) Give two key sizes for AES. (2 marks)
c) What is the size of the square matrix involved? (1 mark)
d) AES uses substitution-permutation network. What is the difference between this network and Feistel network implemented in DES? (2 marks)
e) The following is a simplified state array. In your answer, draw an empty state array and fill in the values after performing shift rows operation. (4 marks)

1A	1B	1C	1D
2A	2B	2C	2D
3A	3B	3C	3D
4A	4B	4C	4D

Question 4

a) "*With defensive programming, we try to reduce the Murphy's Laws effect*". Explain in brief defensive programming and Murphy's Law effect. (2+1 marks)
b) Explain how cross site scripting attacks happen. Given a scenario, there are three parties involved: an attacker, a regular user and a web application that is commonly visited by the regular user. (3 marks)
c) State three methods of validating input syntax. (3 marks)
d) What is input fuzzing? (1 mark)

Question 5

Select p, q	p and q both prime, $p \neq q$
Calculate $n = p \times q$	
Calculate $\phi(n) = (p-1)(q-1)$	
Select integer e	$\gcd(\phi(n), e) = 1;\ 1 < e < \phi(n)$
Calculate d	$de \bmod \phi(n) = 1$

a) Two pair of keys {5,14} and {11,14} are used for RSA encryption and decryption, respectively. Given prime numbers p=2 and q=7, how to generate these two pairs of keys? Show your workout with the information as shown in the figure. (6 marks)
b) You are given a plaintext "E" which is represented with 5. With the keys in (a), find the cipher text in the form of a letter. (2 marks)
c) What are brute-force attacks? (1 marks)
d) What is the good way to counter brute-force attacks in RSA? (1 mark)

End of Page